CLOUDENTITY™

Microsevice Security Mesh For DevSecOps

Summary

The modern cloud architectures use of microservices has many advantages and allows Developers to deliver business software in a Continuous Improvement and Continuous Delivery (CI/CD) way. Despite this industry shift, the market has lacked a tool that allows development teams to natively protect business workloads. Such a tool would need to address security in a microservices or service mesh approach in a way that supports an end-to-end DevSecOps model. The Cloudentity Security Mesh has been architected as microservices and is designed for supporting microservice architecture(s) and integrate with microservices infrastructure. Using Cloudentity, dozens of customers across industries, have realized time to market and development savings of over 20% by empowering enterprise application developers to seamlessly include identity and security into CI/CD to accelerate the DevOps process.

Introduction

Business agility is required for organizations to remain relevant in today's marketplace. According to research from the American Enterprise Institute[1], 88% of Fortune 500 firms from 1955 were replaced by 2016 and the market is better off because of that "creative destruction".

In that timeframe, there have been many examples of companies that remained agile and others that were not able to adapt. Blockbuster failed to transition with the new market and made way for Netflix. GE, on the other hand, successfully transformed from a classic conglomerate to a digital industrial company that's largely defining the future of the Internet of Things. We even see companies that leverage technology to create new markets, such as Uber and Tesla, who are revolutionizing the Transportation and Automotive markets respectively.

To avoid the Blockbuster bust, companies are refashioning themselves as technology companies that provide integrated services in their vertical. For example, CapitalOne no longer refers to itself as a bank but as a technology company providing banking services. And thus, increased their business appetite for agility and digital transformation. This truly applies to the software development process that has changed significantly. Early on we saw the waterfall delivery method, where large monolithic applications and features were planned out in full, ahead of development. Then came the agile scrum delivery method, allowing developers to factor in the challenges that could not be perceived and creating n-tier architecture. Today's agility requirements necessitate businesses move to cloud-based applications and a need to streamline development for CI/CD has brought us the DevOps approach, distributed applications and the proliferation of the use of APIs and microservices.

This level of agility creates huge challenges as organizations work to adapt to new agility requirements. McAfee's, Building Trust in a Cloudy Sky[2], estimated that 93% of organizations utilize cloud services in some form, yet 49% have slowed their cloud adoption due to a lack of cybersecurity skills. VersionOne's

---

[1] AEI, Fortune 500 firms 1955 v. 2016: Only 12% remain, thanks to the creative destruction that fuels

[2] McAfee, Building Trust in a Cloudy Sky, https://www.mcafee.com/us/solutions/lp/cloud-security-report.html

"11th Annual State of Agile"[3] survey, tells us that in the move to an agile development process 94% of organizations practice some form of agile development, yet 80% of organizations report to be at or below the "Still Maturing" phase. Finally, 71% of organizations have "Current or Planned" DevOps initiatives, but current architecture and communication issues slow the process.

Companies need the right development tools for the next phase in moving to a DevOps pipeline. Other tooling such as container orchestration, service discovery, load balancing, request routing and so on has provided layers of abstraction that increase agility and development velocity. It's time for security, more specifically access control and API security, to mature enough to be abstracted into microservices, serverless, containers and cloud-native architectures.

The Case for DevOps – Modern Cloud Architecture

The modern cloud architecture has led to numerous microservices that make up an organizations platforms or products. Often different business groups have different sets of microservices creating their own authentication and authorization logic to secure transactions. This results in a lack of unified security policies which, in turn, leads to a longer time for production release and thus, longer time to market.

One approach that has been used to solve this has been the implementation of an API gateway as a common ingress/egress point to applications. While this can provide a unified security policy, and offload basic security requirements, it loses the flexibility and abstraction that new architectural patterns such as service meshes, serverless functions and multi-cloud provides substituting it for legacy ingress/egress architectural data center style patterns. This contradicts the core tenet of the microservice enablement strategy, which empowers the product development teams to act quickly and deploy solutions rapidly, without being dependent on centralized component configuration.

The ideal approach is to use a micro-gateway that provides the ease and security that legacy perimeter security like API gateways provided for data centers and monolithic applications, adapted to modern microservices and service mesh deployment models. The micro-gateway can be deployed, updated, and configured with each microservice as a singular package. This complements the CI/CD approach needed for DevOps and creates a security service mesh setting the gold standard in the DevSecOps process.

This development tool offloads developers from having to code microservice specific security aspects. Creating a single logical security "pod" that is protected by its dedicated micro-gateway securing the business function by itself. It also ensures constant and equal management of transactional security for all users, services and things. Freeing up development teams to focus on product specific functionality in a truly DevOps manner.

Why CLOUDENTITY™?

The Cloudentity Security Mesh provides the MicroPerimeter™ that is the micro-gateway and session-grid designed for usage with any combination of IAAS, PAAS serverless and on-prem hybrid architectures. It

provides a common Identity platform for users, workloads and things, all designed to accelerate the development workflow for independent product development teams. The MicroPerimeter™ is where identity and cybersecurity converge, forming a secure, frictionless experience for Developers and Users. It provides all the security functionality required for CI/CD in DevOps processes. This is achieved by offloading the transactional security requirements needed to provide inspection, authentication and authorization to microservices and functions. In addition, the

[3] VersionOne's, 11th Annual State of Agile, http://stateofagile.versionone.com/

Cloudentity Security Mesh has real-time risk profiles, step up transactional authentication, risk mitigation responses and a full compliance audit trail.

The MicroPerimeter™, unlike a centralized API gateway, protects one microservice or small domain of microservices. Its purpose is to handle utility security requirements such as…

- Strong Authentication of services and users
- Dynamic Coarse and Fine-Grained Authorization
- OAuth, SAML, OIDC
- Transaction Throttling
- TLS and Secret Off-Load
- Brute-force Protection
- Service Discovery
- Service Configuration
- Canary Routing
- Distributed PDP/PEP

The MicroPerimeter™ also has a pluggable architecture that enables each incoming request and outgoing response to be subject to custom transformation performed by configurable plugins. All possible because the MicroPerimeter™ has a minute footprint allowing it to be deployed to protect as a micro-API-gateway, or next to the microservice. Otherwise known as a sidecar approach.

The Cloudentity Security Mesh also includes the TrUST Authorization Engine™ which measures real time transactional risk between the services, users and things protected. The solution can assess and evaluate risk on a transactional basis and provide dynamic authorization flows to mitigate the risk.

The TrUST engine's dynamic authorization is available for every transaction, from the initial User authentication to every application to application transaction, while maintaining user context, solving complex microservices security and audit issues while ensuring the highest levels of security and providing security and visibility to the inter-service transactions that make up 80% of transactions today.

Further still, each transaction creates a comprehensive digitally signed audit trail from authentication to data access via unique individual transaction IDs and verified claims available to applications, microservices, APIs, containers and server-less functions for frictionless fulfillment of governance and compliance requirements.

Leverage Existing Identity and Security Platforms

One might ask if utilizing the Cloudentity Security Mesh would require replacing an existing identity platform if one is already in use. The simple answer is no, mainly due to another major advantage of microservice architecture. Although Cloudentity offers a full suite of identity services, organizations can choose what microservices they need since each service is independent. Think of it as an à la carte offering of identity services. If an organization is seeking to utilize the MicroPerimeter™ to offload transactional security through authentication and authorization yet would like to leverage an existing identity platform that can be done.

Most identity platforms are largely still monoliths themselves preventing them from participating effectively in microservice environments. Despite that it may not be optimal to have users establish a new identity or to change to a new authentication workflow. Cloudentity supports integration with existing legacy identity platforms through our Token Exchange Service. This service allows session tokens to be created or verified.

Existing security platforms can be leveraged as well. For instance, the platforms flexibility and our partnership with Imperva allows the Cloudentity MicroPerimeter™ and TrUST Engine™ to integrate with Imperva SecureSphere. In this case if the TrUST Engine™ detects higher risk transactions, the Cloudentity MicroPerimeter™ pauses the transaction and sends it to Imperva SecureSphere for additional inspection. The inspection result, updates the risk profile determining the next required steps for mitigating or completing the transaction.

Conclusion

The Cloudentity Security Mesh ensures that enterprises can develop one security strategy to consistently deploy across an entire product or organization. Application specific security for all users, services, and things with an individual MicroPerimeter™ allowing for per-transaction authentication and per-resource authorization. This is accomplished by decoupling API, microservice and container security from the business function and using identity and intelligent authorization as the center point. Empowering enterprise application developers to seamlessly integrate identity and data security to accelerate the DevOps process creating a service mesh that is the gold standard in DevSecOps.

T. Rowe Price is a good example of a customer who has implemented the Cloudentity Security Mesh. Blake Kizer, Lead Security Engineer at T. Rowe Price said, “The implementation felt easy…Everything worked out of the box, what was guaranteed to work did work”.

The Cloudentity Security Fabric has enabled a variety of customers across industries, to realize a 20% reduction in time to market and development.

About CLOUDENTITY™

Cloudentity is a leader in providing a real-time self-healing identity and security layer to cloud-native applications by leveraging Identity and Fraud Management and was recently named in Gartner’s 2017 “Cool Vendor” report. We unleash organizations to deliver Secure Digital Transformation by delivering dynamic real-time authentication, authorization and management across users, services, and things. Utilizing Identity at the heart of everything we do, we drastically reduce application-owners time to market by offloading cybersecurity and identity requirements allowing developers to focus on game changing business applications in a comprehensive SecDevOps manner.

Cloudentity is trusted by dozens of customers in Finance, Insurance, Government, Retail, and Healthcare, including leading companies like Blue Cross-Blue Shield, Reliance Industries, PG&E, Crowdstrike, T Rowe Price and Standard Insurance Corp.

*Contact the Cloudentity team today for a demo or download a trial from website **www.cloudentity.com***

CLOUDENTITY™

Cloudentity
2815 2nd Ave, Suite 390
Seattle, WA 98121
Tel 1-888-796-8341
www.cloudenity.com